Contribution to the DOE National Collaboratories Program Investigator's Meeting, August 10-12 at ANL.

An Architecture for One Time Passwords and Cross-site Grid Security

Von Welch (vwelch@ncsa.uiuc.edu), Jim Basney (jbasney@ncsa.uiuc.edu), Frank Siebenlist (franks@mcs.anl.gov)

Recent security attacks have pointed to vulnerabilities in multi-use authentication secrets (e.g., static passwords). These attacks have not been limited to network sniffing, but instead have involved the introduction of Trojan services and modifications to kernels on multi-user or compromised computers in order to capture keystrokes directly. The success of this strategy has meant that previous tools for protecting passwords as they pass over the network (e.g., Kerberos, SSH) are vulnerable, as the attackers can gain access to a user's password as it is being typed.

These attacks are leading many sites to investigate hardware-based one-time password (OTP) solutions for authentication. The solutions allow authentication of an individual without that individual ever being required to type an authenticating pass phrase more than once, therefore greatly reducing the effectiveness of pass phrase sniffing.

However, adoption of OTP-based solutions poses several significant challenges for distributed and Grid computing:

1. Use of a single OTP hardware token at multiple sites is currently very difficult even if those sites have chosen the same token vendor and impossible if they have chosen different vendors. This would result in users having to carry a keychain of these tokens to access multiple sites.
2. Support of single sign on (accessing multiple resources with a single authentication) is to a large degree an unexplored area.
3. Integration of OTP and Grid security based on X.509 identity certificates is also unexplored.

We believe a architecture that integrates Grid security and OTP can solve all three of these problems in such a way that combines the benefits of both OTP's protection against reuse of pass phrases and Grid security's cross-site single sign-on. We believe it is time to change the fundamental nature of how Grid credentials are managed, from a user-based model to a model based on Grid credential services that can be deployed in datacenter settings and managed by professional administration and security staff. The architecture of such a Grid credential storage service would include important features as the following:

- Users do not manage their own long-term credentials. Instead, they authenticate to the Grid credential storage service and receive back a short-term credential. (either an X.509 identity or proxy credential).
- The service authenticates the user using a pluggable authentication module, so that each site can deploy the service can integrated with the site's authentication mechanism of choice, including OTP mechanisms.
- The service returns a short-lived credential (either an X.509 identity or proxy credential) to the user to enable their access to the Grid. This credential is short lived (under administrative control of the credential service administrator), after which time the user

must contact the credential service again to obtain a new credential. This short-lived credential can be used to authenticate at different services during its lifetime to allow single sign-on, while allowing the issuing site to control the lifetime of the credential according to their comfort level.

- Sites can easily choose to accept credentials issued by other sites, allowing support of cross-site distributed and Grid computing.

We believe there are a number of side benefits to this approach:

- It relieves the users from the process of acquiring and managing long-term X.509 credentials, a burdensome and error-prone process for most users.
- Relying parties typically have more trust in professional operations staff to manage long-term credential than users. A Grid credential service can be secured using techniques developed for similar services such as Kerberos KDCs.
- Accesses to the credentials can be audited and monitored to detect misuse during or after the fact.
- Users can access their credentials from any location, granting a greater freedom of mobility, while avoiding the need to copy credentials in an ad hoc manner over the network (a potentially insecure process).
- The resulting short-term credential is compatible with existing Globus Toolkit Grid software.

Such a system is currently in collaboration between NCSA, ANL and NERSC. NCSA is working on an implementation of such a Grid credential service built on the current MyProxy service for credential management. This is being done in close collaboration with NERSC, who is providing requirements and acting as the primary testing grounds. ANL is providing expertise and support in the form of needed changes to the underlying Grid security libraries in the Globus Toolkit.